

(12) UK Patent Application (19) GB (11) 2 291 237 (13) A

(43) Date of A Publication 17.01.1996

(21) Application No 9513815.2

(22) Date of Filing 06.07.1995

(30) Priority Data

(31) 9413614

(32) 06.07.1994

(33) GB

(71) Applicant(s)

Philip Martin Ashley
Whiddon Hall, Burley Lane, Menston, ILKLEY,
LS20 7EU, United Kingdom

(72) Inventor(s)

Philip Martin Ashley

(74) Agent and/or Address for Service

Forrester Ketley & Co
Forrester House, 52 Bounds Green Road, LONDON,
N11 2EY, United Kingdom

(51) INT CL⁶

G07F 7/10

(52) UK CL (Edition O)

G4H HTG H1A H13D H14A H14B H14D
U1S S1727 S2271

(56) Documents Cited

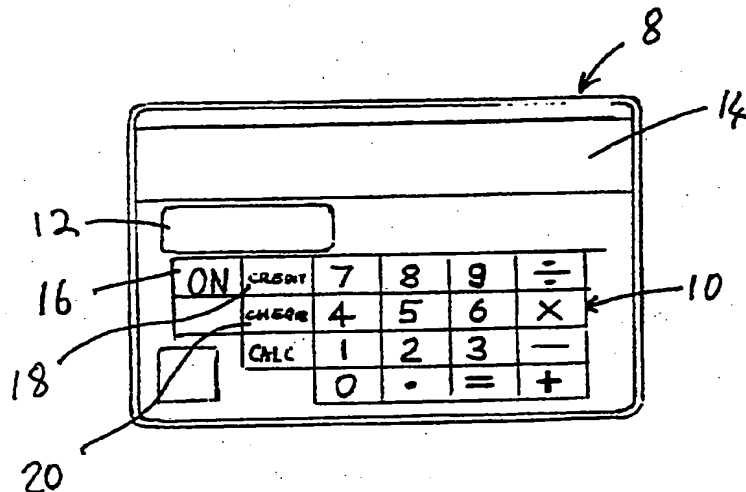
GB 2272552 A GB 2201125 A WO 86/03040 A1
WO 83/03018 A1 WO 82/03484 A1 US 4868376 A

(58) Field of Search

UK CL (Edition N) G4H HTG
INT CL⁶ G07F 7/10

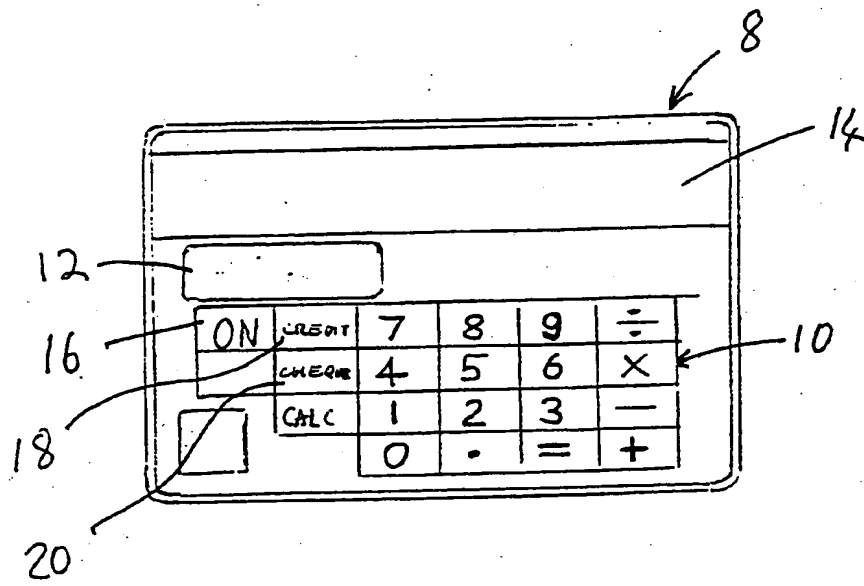
(54) Credit card or the like and system utilising same

(57) A credit card, charge card or the like is in the form of a "smart card" having a keyboard by which the legitimate owner can make a secret entry which will activate the card selectively, for the period of the intended transaction only, to output data via magnetic data means 14 readable by a magnetic stripe reader and via a display 12. In a variant, the "smart card" has stored therein in electronic data form, a visual image of the legitimate card holder and which is convertible to a corresponding visual image by complementary apparatus e.g. at a point of sale.



GB 2 291 237 A

- 1/1 -



2291237

PATENTS ACT 1977

DESCRIPTION OF INVENTION

Title: "Credit card or the like and system utilising same"

THIS INVENTION relates to a device which may be embodied as a credit card, charge card, store card, debit card, cheque guarantee card, identification card or the like, which items are herein referred to collectively as "cards of the kind specified". The invention also relates to systems, such as automatic teller systems, utilising cards of the kind specified.

It is among the objects of the invention to provide a card of the kind specified which allows a substantial increase in security against fraud, in systems using such cards and which nevertheless can be manufactured inexpensively and which is compatible with existing system hardware.

According to one aspect of the invention, there is provided a card of the kind specified which incorporates entry means and data output means readable by a complementary reading device, but which data output means is arranged to be activated selectively, for a limited period only, by circuitry within the card upon the predetermined coded entry being made, via said entry means, by the user.

Preferably said data output means comprises magnetic data means readable by a magnetic stripe reader.

Preferably the card incorporates a battery, microprocessor means, keypad means forming said entry means, and a plurality of electromagnetic current carrying

elements affording said magnetic data means and adapted to be supplied with current from said battery, under control of said microprocessor means, for said limited period after entry of the appropriate coded entry to said processor means via said keypad means.

The card may incorporate display means, such as an LCD display, driven by said microprocessor means.

An embodiment of the invention, as applied to a credit card, is described below, by way of example, with reference to the accompanying drawing which shows one face of a card embodying the invention.

The card shown at 8 in the drawing is a so-called "smart card" which incorporates a microprocessor, a battery powering the microprocessor, a membrane key pad 10 on one face of the card and providing entry means whereby data and instructions for the microprocessor may be entered by the user. The card 8 may also incorporate, as shown, an LCD display 12 wherein entries made can be checked by the user. The card further incorporates magnetic data means, located in a region covered by a strip of pressure sensitive metallic conductor 14, and which magnetic data means is capable of simulating, for magnetic stripe readers such as are conventionally provided at automatic teller machines, point of sale stations and the like, the magnetic stripes conventionally provided on credit cards and the like. Such magnetic stripes conventionally carry, in the form of a pattern of magnetisation, an identification code unique to the card concerned. The magnetic data means, by way of example, may comprise a plurality of flat electromagnetic "coils" formed by patterns of metallisation on an insulating substrate of the card, for example in "printed circuit" form, these coils being covered by a thin

insulating layer covered, in turn, by the pressure sensitive metallic conductor 14.

The opposite face of the card may simply bear markings or designs identifying the issuing authority and bearing the card holder's name, for example.

As indicated below, the pressure sensitive conductor 14 may function, in conjunction with contact pads on the "printed circuit" underlying the conductor 14, as a switch which is closed when the conductor 14 is pressed into the card by the reading head of a magnetic stripe card reader, to indicate to the microprocessor incorporated in the card that it is being "swiped" through such a magnetic stripe reader, and the card may be arranged to activate its magnetic "coils" only during such swiping and for a period no longer than such a "swipe" requires, thereby minimising power consumption and making more difficult unauthorised deciphering of the card.

Further details of the card will be evident from the following description of the mode of operation thereof.

In use of the card 8 or a credit card, to pay for purchases at a cashier station in a store, for example, the card user turns on the card by pressing an ON switch or key 16 on the keypad 10. The user then enters a Personal Identification Number (PIN), in the form of a code of X digits (say 4) via the membrane keyboard 10. The card remains active for a predetermined length of time (say 3 minutes). After entry of the code, the microprocessor matches the user's code with that of a pre-stored code (which is stored in read only memory). If the two codes are identical, then the microprocessor will allow the card holder's data (card number, expiry date or any other pre-

stored information) to be displayed on the LCD panel for examination by the cashier. Furthermore, if the card is "swiped" through an electronic card reader or inserted into an automatic teller machine (the microprocessor detects these devices by feedback from the pressure sensitive conductor 14), the card holder's data relevant to a transaction is transmitted via said magnetic data means, such as printed circuit "coils" to the magnetic card reader, through the pressure sensitive conductor 14. As the pressure sensitive conductor 14 is in contact the magnetic head of the card reader during the swipe action, the data is therefore uploaded (transmitted) to the ATM (automatic teller machine), electronic point of sale equipment or modem associated with the card reader, thus enabling examination of the said data and allowing a secure transaction to be made.

Should the Personal Identification Number be incorrectly entered the user may re-attempt the operation for a predetermined number of attempts (say 5) within a given period of time (say three minutes). If the user attempts a greater number of attempts to enter the code within the predetermined period of time, all data within the card will be destroyed. Thus, the card can never be used without first entering the correct code.

The card will bear only the user's name and have no card number printed externally, thus increasing security.

The card will be initially programmed by the issuing authority and cannot be reprogrammed, as the microcontroller employed in the design is an OTP (one time programmable). However, it may be possible for the user to modify the PIN, but only after inserting the PIN encoded by the issuing authority. This information will be stored in

E2EPROM (electronically erasable electronically programmable read only memory).

A basic electronic calculator may also be incorporated into the card to assist with day to day transactions.

The basic components required to produce the card are a microprocessor or microcontroller, read only memory, electronically erasable read only memory (E2EPROM), a membrane keypad controller, a liquid crystal display (LCD-panel), a battery, a pressure sensitive conductor strip, a custom designed plastic card.

TYPICAL USER OPERATION

In Store Transactions - (Use as credit card, debit card or store card.

1. Switch on card.
2. Enter code into card. Display flashes "SWIPE".
3. Pass to cashier. Cashier swipes card through card reader.
4. Sign for goods as normal.
5. Transaction complete.

Telephone transactions - (Credit card transactions)

Telephone transactions are made as follows:

1. Switch on card.
2. Key in code number.

3. Request card number and expiry date.
4. Card number and expiry date are displayed on the LCD panel.
5. Give information to the retailer over telephone.
6. Transaction complete.

It may be possible to display the user's "signature" after the code has been entered for verification, this would need to be scanned in by the issuing authority, then stored in Read Only Memory. In reality this is unnecessary.

ATM Transactions

1. Switch on card.
2. Enter code into card and insert in ATM.
3. Enter code into ATM (for added security this may be an additional, different code).
4. Request cash from ATM.
5. Remove card. Transaction complete.

ATMs can be made to recognise "smart credit cards", so the number need not be entered twice.

Cheque Guarantee Transactions

1. Write out the cheque.
2. Switch on card.

3. Enter Personal Identification Number.
4. Pass cheque book and card to cashier.
5. Cashier writes number on cheque.
6. Transaction complete.

Enhancements

ATM Transactions.

1. In addition to PIN number, the amount in cash required could also be entered into the card then automatically tendered. This would speed up queues at ATMs. This would require a software modification to the ATMs.
2. In-built calculation functions, current account balance, credit limit, amount remaining etc. could all be displayed if desired.
3. If banks could be made to agree, all credit, charge and security cards could be programmed onto one card.

Thus, the keypad 10 shown in the drawing includes a key 18 to be pressed by the user (after successful completion of the PIN code as described above) to cause the display 12 to display, briefly, the credit card number. A key 20 can likewise be pressed to cause the display 12 to display the user's cheque card number. As these numbers are not otherwise displayed on the card, and are not otherwise discoverable by third parties who are unable to activate the card without a knowledge of the PIN number, it is not possible for a thief to use the card and debit purchases etc. to the legitimate owners accounts.

The card described can form the basis of a credit card fraud prevention system which is a low cost solution which should almost totally eradicate all credit card fraud. The system is virtually foolproof, easy to use and manufacture, and requires no modification to the existing systems employed within banks, stores, garages etc. The system is equally effective with credit, charge, store, debit, cheque guarantee and cash withdrawal cards.

In a variant of the card described, the magnetic data means may be replaced by or supplemented by, some other means for passing data from the card to a card reading device. For example the card may have electrical contacts for engagement with contacts of a card reading device, allowing data to be transferred from the card to the card reading device in the form of electrical signals, the card again being so arranged that such data is only made available to such reading device for a limited period after a valid entry by the user.

In variants, the "Smart Card" may, in addition to or in place of the magnetic data means, bear electrical contacts to facilitate interfacing with "Electronic Point of Sale Terminals", "Automatic Teller Machines" and the like.

An additional application of the keyboard and display is that of "Programmable transactions". This is, in the context of a credit card, the ability to program limits of currency requested from an "ATM", "EPOS" terminal or the like. Individual amounts of "currency" may be assigned to a specific and programmable "Personal Identification Number".

In a further variant, positive identification of a card holder may be provided by means of visual image matching in conjunction with interrogation by way of a computer controlled Electronic Point of Sale device.

In this variant "positive identification" of a card holder is provided in a friendly manner with maximum security and reliability.

In this variant, a digitised image of the card holder, (for example of the face of the card holder) compacted to save memory and encrypted for security purposes, is stored within the card in Read Only Memory (ROM) or Random Access Memory (RAM). Furthermore, details secret and/or proprietary to the card holder are also stored in the card memory.

In use, this variant will be tendered for payment, and inserted into an aperture in an "Electronic Point of Sale" terminal designed specifically to interface with the card. The "EPOS" terminal uploads the digitised image of the card holder from card along with other required data. The image of the card holder is displayed on the video screen of the "EPOS" terminal. The "EPOS" operator can now make a positive identification of the card holder by matching his/her profile to that of the image displayed on the video screen. Furthermore, the software controller of the "EPOS" terminal is programmed to superimpose onto video display, questions, chosen randomly, pertaining to the card holder proprietor and the answers to which comprise secret information stored in memory on the card. The operator must verbally convey the query displayed to the card holder, and enter the response by way of the keyboard controller connected to the "EPOS" terminal. If the response to the question(s) matches the data stored, then

a transaction may be approved by the "EPOS" terminal. If the response is negative, then the transaction may be declined, and the card returned or destroyed.

CLAIMS

1. A card of the kind specified which incorporates entry means and data output means readable by a complementary reading device, but which data output means is arranged to be activated selectively, for a limited period only, by circuitry within the card upon the predetermined coded entry being made, via said entry means, by the user.
2. A card according to claim 1 wherein said data output means comprises magnetic data means readable by a magnetic stripe reader.
3. A card of the kind specified which incorporates entry means and data output means readable by a complementary reading device and which has stored therein, in data form, a visual image of the card holder.
4. A card of the kind specified, substantially as hereinbefore described with reference to and as shown in the accompanying drawings.
5. Any novel feature or combination of features described herein.

12

Patents Act 1977
Examiner's report to the Comptroller under Section 17
The Search report)

Application number
 GB 9513815.2

Relevant Technical Fields

- (i) UK CI (Ed.N) G4H (HTG)
 (ii) Int CI (Ed.6) G07F 7/10

Search Examiner
 M J DAVIS

Date of completion of Search
 11 AUGUST 1995

Databases (see below)

- (i) UK Patent Office collections of GB, EP, WO and US patent specifications.

Documents considered relevant following a search in respect of Claims :-
 1-2, 4

(ii)

Categories of documents

- | | |
|--|---|
| <p>X: Document indicating lack of novelty or of inventive step.</p> <p>Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.</p> <p>A: Document indicating technological background and/or state of the art.</p> | <p>P: Document published on or after the declared priority date but before the filing date of the present application.</p> <p>E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.</p> <p>&: Member of the same patent family; corresponding document.</p> |
|--|---|

Category	Identity of document and relevant passages	Relevant to claim(s)
X	GB 2272552 A (HALPERN ET AL)	1
X	GB 2201125 A (DE LA RUE)	1
X	WO 86/03040 A1 (INTELLICARD)	1
X	WO 83/03018 A1 (ERICSSON)	1
X	WO 82/03484 A1 (BENTON)	1
X	US 4868376 (LESSIN ET AL)	1, 2

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).